https://dx.doi.org/10.22161/ijaers.4.8.6 *ISSN: 2349-6495(P) | 2456-1908(O)*

A Secure IoT Data Integration in Cloud Storage Systems using ABAC Access Control Policy

Ismail Chahid, Abderrahim Marzouk

IR2M Laboratory, Faculty of Science and Technology, University Hassan 1st Settat, Morocco

Abstract— *Internet of Things has become one of the most emerging technologies now days, which is growing rapidly in the telecommunications field. It is as a network of physical objects, peoples, vehicles, buildings, and other items, which are having a unique identity and are able to interchange data using embedded electronics, sensors, and software equipment to reach common goals. The large scale of real time data collected and exchanged between objects in IoT grows exponentially which represent a big challenge in term of storing and processing. Cloud Computing has emerged as a key technology to solve the problem of IoT data storage and processing by offering multiple choices of resources provided by cloud service provider, including storage, processing, memory and network bandwidth. Nevertheless, as many other technologies, Cloud computing has some issues regarding IoT data storage. One of the major issues is Security and Privacy. In this paper, we will present a proposed architecture for a Secure IoT data integration in Cloud Storage Systems.*

Keywords— Cloud Computing; Internet of Things; Security; Data.

I. INTRODUCTION

In the recent years, Internet of Things (IoT) has become one of the most promising technologies in the telecommunication field. It represent a new paradigm in which interconnected and heterogeneous entities such as physical objects, peoples, vehicles, devices, buildings and other objects are having a unique identity (ID) and are able to interchange data using embedded electronics, sensors, and software equipment to reach common goals [1]. This new step in technology sector will have a high impact on different areas including smart homes, assisted living, e-health, industrial manufacturing and environmental monitoring. The main technologies parts involved in Internet of Things are Wireless Sensor Networks (WSN), Radio-frequency identification (RFID), machine-to-machines interfaces (M2M), micro-electromechanical systems (MEMS) and Internet. All this technologies combined with different entities in IoT environment will increase the amount of data collected exponentially which represent a big challenge in term of processing and Storing. Cloud Computing appear to be an ideal choice to solve the problem of processing and storing data collected from different IoT devices [2], since it provide a multiple choice of resources including high performance processing, storage, memory and network bandwidth that are accessible on demand anywhere [3]. However, Cloud Computing technology comes with some issues that are Security and Privacy concerns [4]. Many organizations, companies and individuals are using sensitive and confidential data in their transactions. This data is collected from IoT devices and moved into cloud storage to be processed using different computing techniques like virtual machines. Many security challenges can be encountered during this process like accessibility vulnerability, and virtualization vulnerability. which makes it hard for organisations to adopt this technology due to previous mentioned concerns. This paper is organized as follows. In section 2, we present the previous released research that deal with the topic of IoT data security in Cloud Storage. Section 3 discuss the IoT architecture and the authentication of IoT devices to the Cloud. Moreover, in section 4 we discuss the ABAC Access Policy and finally we present the proposed architecture for IoT Data integration to the Cloud.

II. RELATED WORK

Security issues is on of big concerns in term of storing processing and managing data in both IoT and Cloud environment. In [5] authors presented a survey on secure integration of IoT and Cloud Computing, and then they proposed a model for securing this integration. A secure storage system was proposed for storing IoT data in [6], the authors applied a Role Based Access Control policy (RBAC) combined with AES/RSA encryption to manage authenticity and data security, but Role-based access controls (RBAC) may not suffice in the IoT because of the lack of flexibility.. In [7] an authentication model was described based on different access use case scenarios in IoT Clouds. A multi-layer cloud architectural model was proposed in [8] for IoT-based smart homes, the main idea focus on the development of a Public cloud that collect data from different private cloud vendors using Ontology-based security service framework.

https://dx.doi.org/10.22161/ijaers.4.8.6 *ISSN: 2349-6495(P) | 2456-1908(O)*

III. IOT DATA INTEGRATION IN THE CLOUD

A. Internet of Things Architecture

IoT architecture can be represented with four categories of interconnected systems such as things, gateways, network and cloud as showed in Figure 1.

Things: Today large amounts of things are found in industrial and commercial settings, it is also in users mobile and home. Already, cars, device sensors, and mobile phones are accessing the Internet through broadband wireless networks. IoT technology solution requires intelligent things capable of filtering and managing data locally and connecting to gateways easily.

Gateways: The majority of existing things are not capable to connect to the internet to share data with the cloud because of their design. To solve this issue, gateway act as intermediate between internet and things.

Network Infrastructure: Internet is a complex system of interconnected IP networks that links billions of computers together. Network infrastructure comprises gateways, routers, repeaters, switches and other devices that controls the data traffic and connect with cable and telecom networks operated by different service providers

Cloud: Cloud contains huge number of interconnected virtualized servers and standard servers connected together. To support the IoT environment cloud infrastructure runs different applications, which are capable to analyse the data collected from different devices and sensors to make the correct decision.

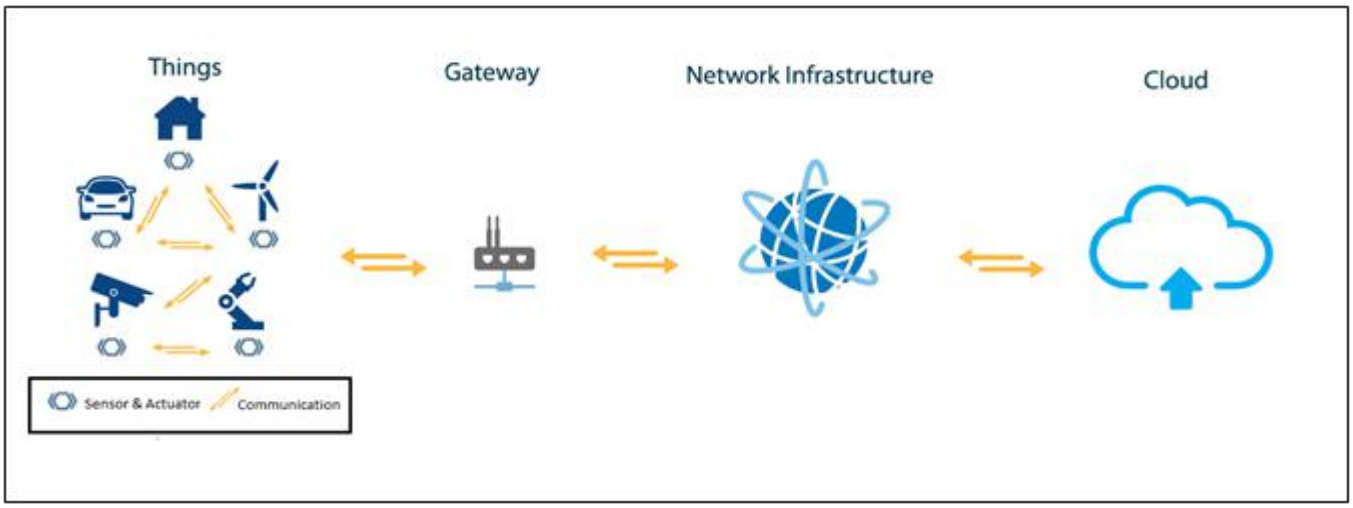

Fig. 1: IoT Architecture

B. Cloud Computing Architecture

According to the official NIST definition, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Cloud Service Providers (CSP) offer their "services" according to standard models defined by NIST, are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) Figure 2.

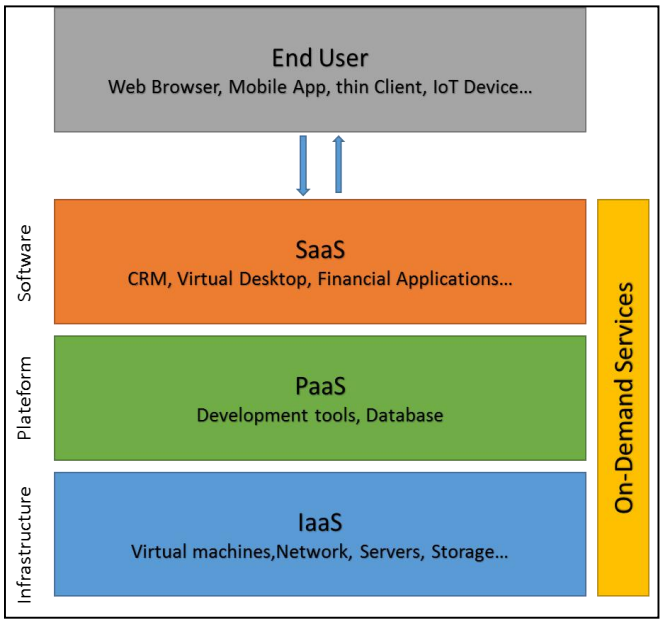

Fig. 2: Cloud Computing Layers

https://dx.doi.org/10.22161/ijaers.4.8.6 *ISSN: 2349-6495(P) | 2456-1908(O)*

C. Authentication for IoT Clouds

Nowadays, Cloud Computing can provide access to IoT-based resources through special designed applications with specific interconnected structures. Thus, a new iteration in the "as-a-service" model is added to Cloud Concept, which is IoT as a Service or simply (IoTaaS). This new model requires a complex authentication scheme. Authentication refers specifically to verifying the identity of a device. It aims to prove that all entities are what they claim to be. This ensures that communications are only transmitted to the intended recipient; The authentication completely reassures the recipient on the origin of the communication. In the IoT universe, several scenarios are possible: authentication of devices on cloud services, users on devices, objects on objects.

In IoT development field, Authentication standards are a major requirement to execute operations in the efficient way. There is a variety of competing standards. One of them is Fast Online Identity (FIDO) alliance and the other one is M2M. They are both growing authentication and access architectures intended for all IoT markets.

To maintain security, trust, privacy and confidentiality of the integrated data, Internet of Things requires a solid and proven approach.

PKI infrastructure is an interoperable and standard-based technology that has been used in IoT. It comes with a specific scheme to provide main security assessments like privacy data integrity and authentication [9]. The design of PKI infrastructure makes it easily adapted for IoT requirements in term of diversity, velocity and volume. There are many models of integration of the PKI Infrastructure in IoT, one of the models is the hardware based cryptographic device TPM which is a ship that needs to be integrated to the device.

Enabling strong identities at the hardware level protects against identity theft and the compromise of keys that would endanger the entire interconnected system. If a change occurs, the entire ecosystem is notified and the administrators can respond accordingly.

IV. ABAC ROLE BASED ACCESS POLICY

Access control is based on the identity of a user requesting execution of a capability to perform an operation (e.g., read) on an object (e.g., a file). This can be done directly either as in Discretionary Access Control or Mandatory Access Control or through predefined attribute types, such as roles or groups assigned to that user as in Role Based Access Control or RBAC.

Role-based access controls (RBAC) by themselves may not suffice in the IoT because they are not flexible enough. An RBAC-only system would increase risks in IoT systems and services that possess the following characteristics:

- Unpredictable environments: IoT services within unpredictable environments, such as those environments dealing with many people at once. Where crowd dynamics and emotions can create responses to different conditions that are very hard to project.
- Contrary functions: IoT services with dramatically different, or even opposite, functional requirements under abnormal versus normal conditions—for instance, a fire door during an actual fire (abnormal condition) that must open, versus the same door under non-fire conditions that must sound alarms and not open easily.

RBAC cannot effectively account for these sorts of properties alone, and in the IoT, with the increasing prominence of the logical-kinetic/cyber-physical interface, attributes will play an important role in authorization exercises.

Attribute-based access control (ABAC) is an access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions [10].

ABAC has three main functional points, which is as follows:

The PEP or Policy Enforcement Point: is a component that serves for protecting apps & data in which ABAC is applied. The PEP inspects the request and describe the user's attributes to the Policy Decision Point PDP.

The PDP or Policy Decision Point is the component that makes the determination of whether a user's request is authorised or not by evaluating incoming requests against policies it has been configured with. The PDP returns a Permit / Deny decision. The PDP may also use PIPs to retrieve missing metadata

The PIP or Policy Information Point serves as the retrieval source of attributes and bridges the PDP to external sources of attributes e.g. LDAP or databases.

The proposed architecture for the authentication of things in IoT-Clouds is a combination of ABAC Technology and PKI Infrastructure (Figure 3). It forces a smart object in IoT to pass a double check authentication system to ensure that the data is collected from the correct IoT object and not from a fake one. For the users that needs to get access the IoT data stored in the cloud, we used another multi authentication factor which is the mobile two factors authentication MPTFA [11].

https://dx.doi.org/10.22161/ijaers.4.8.6 *ISSN: 2349-6495(P) | 2456-1908(O)*

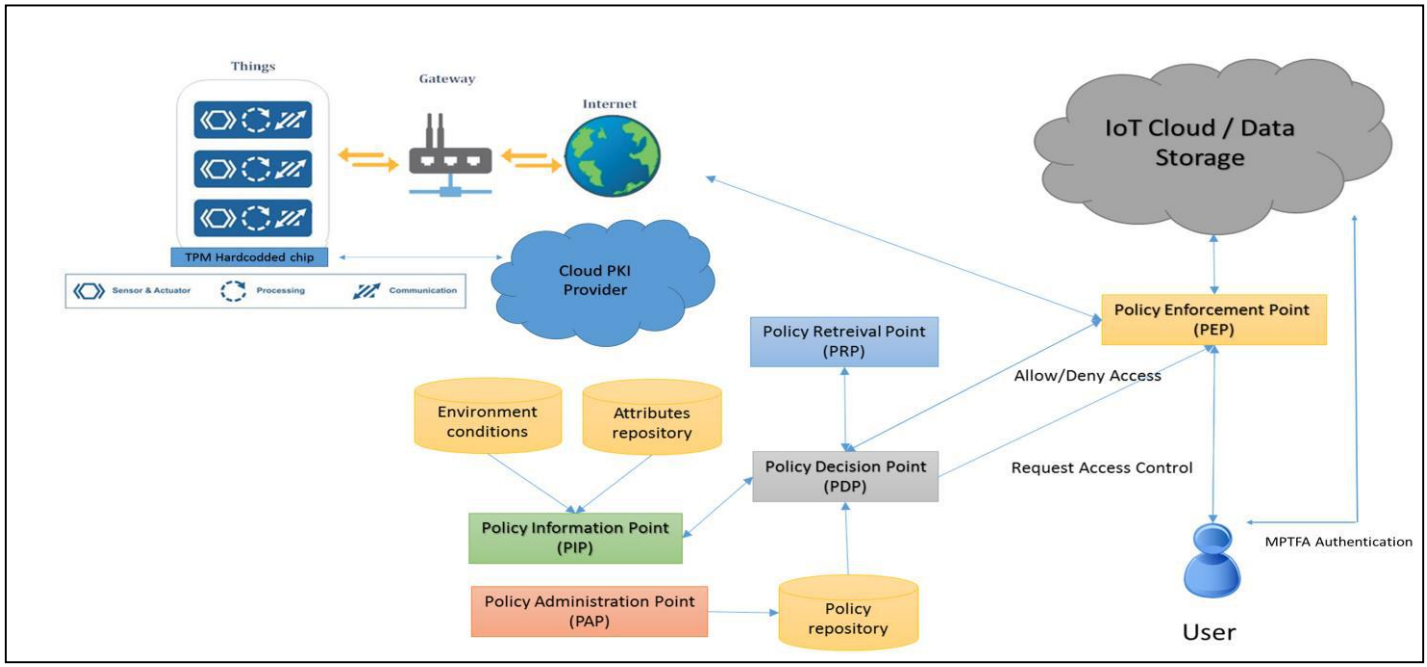

Fig. 3: Proposed Architecture

IV. CONCLUSION & PERSPECTIVES

In our proposed architecture, we tried to make it possible for storage systems in IoT-Cloud infrastructures to ensure that data collected from things and smart objects is authentic and secure by combining three different authentication technologies: ABAC Access Control, PKI Infrastructure system, and MPTFA.

In our future work, we will try to implement an adoptable cryptosystem in the proposed architecture to increase the security level in cloud storage systems.

REFERENCES

[1] Luigi Atzori , et al The Internet of Things: A survey, doi:10.1016/j.comnet.2010.05.010

[2] The intel IoT platforme, white paper, intel 2015

[3] NIST SP 800-145, The NIST Definition of Cloud Computing, 2011

[4] Amit SangroyaSaurabh Kumar Towards Analyzing Data Security Risks in Cloud Computing Environments, DOI: 10.1007/978-3-642-12035-0_25

[5] C Stergiou, et al., Secure Integration of IoT and Cloud Computing, Future Generation Computer Systems (2016), DOI: 10.1016/j.future.2016.11.031

[6] Jayant D. Bokefode et al., Developing A Secure Cloud Storage System for Storing IoT Data by Applying Role Based Encryption. doi: 10.1016/j.procs.2016.06.007.

[7] Luciano Barreto et al., An Authentication Model for IoT Clouds, DOI: 10.1145/2808797.2809361.

[8] Ming Tao, Jinglong Zuo et al., Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes, DOI: 10.1016/j.future.2016.11.011

[9] Aysha Albarqi et al, Public Key Infrastructure: A Survey Journal of Information Security, 2015, 6, 31-37
TPM

[10] Guide to Attribute Based Access Control (ABAC) Definition and Considerations, NIST Special Publication 800-162,

[11] Ayu Tiwari, Sudip Sanyal, Ajith Abraham, Svein Johan Knapskog, Sugata Sanyal, "A Multi-Factor Security Protocol for Wireless Payment – Secure Web Authentication Using Mobile Devices", *IADIS, International Conference Applied Computing*, pp. 160- 167, 2007.